



# Detect Safe Browsing (DSB)

USER MANUAL

OPERATING SYSTEM: ANDROID

v4.1.0

# Content

## **4 Focus**

### **Detect Safe Browsing**

- 5 Introduction
- 5 System Requirements

### **DSB Console Operation**

- 6 Scanning
  - 7 Threat-free device
  - 8 Malware attacks
  - 9 Pharming attacks
  - 10 Marking suspicious entries as trusted
  - 12 Cleaning your device
- 13 Reports
- 14 Protected Sites
  - 15 Adding predefined protected websites
  - 16 Adding personal protected websites
  - 19 Editing protected websites

### **Web Protection**

- 20 Web Address
- 22 Reporting a URL
- 23 Blocking a URL
- 24 Unblocking a URL
- 25 Accessing the Main Menu

### **Monitoring applications**

- 26 Malware notifications
- 27 Certified application notifications

# Content

## Application Configuration

28	Advanced Settings
30	Trusted entries in the Host file
30	Sites unblocked by the user
32	Help
32	Version

The **Detect Safe Browsing** *User Manual* provides information about the terms and concepts applied by **DSB for Android**. This document presents the general features of the product and lists its functionalities and component elements.

# 1 Detect Safe Browsing

## *Introduction*

**Detect Safe Browsing (DSB)** from **Easy Solutions** is an innovative tool created to protect the final users from the electronic fraud modalities commonly used on the Internet.

Within the protection capabilities of the application, you will find system the scanning feature and the Internet connection analysis performed through the operating system browser. Such scanning identifies two possible attacks:

- **Phishing:** Web site impersonation performed by a non-authorized third party to get confidential information for criminal purposes.
- **Pharming:** Manipulation of system information performed by non-authorized users, who re-direct the access from real web sites to fake sites and thus commit fraud.
- **Malware:** Malicious software designed to affect the integrity of a device.

If **Detect Safe Browsing** identifies any of these attacks, it will block the threat and inform the user about the security incident.

Every time a security incident occurs, you will be able to report the threat to the Easy Solutions laboratories so that it can be analyzed and, therefore, the security level of your system will constantly increase. Consult the [DSB Configuration](#) section to activate this option.

## *System Requirements*

To use **Detect Safe Browsing** for the **Android** platform, your device must meet the minimum system requirements below.

- Operating System: Android 2.2 or higher
- Internet connection.

## 2 DSB Console Operation

### Scanning

Start the device analysis:

1. Select the *Scan* [1] option and tap on the *Analyze Device* [2] button.



2. Then, the scanning process looking for suspicious records in the system will start.
3. At the end of the scanning process, the application will inform you of the result: [Threat-free device](#), [Malware attacks](#) or [Pharming attacks](#).

## DSB Console Operation

*Threat-free device*

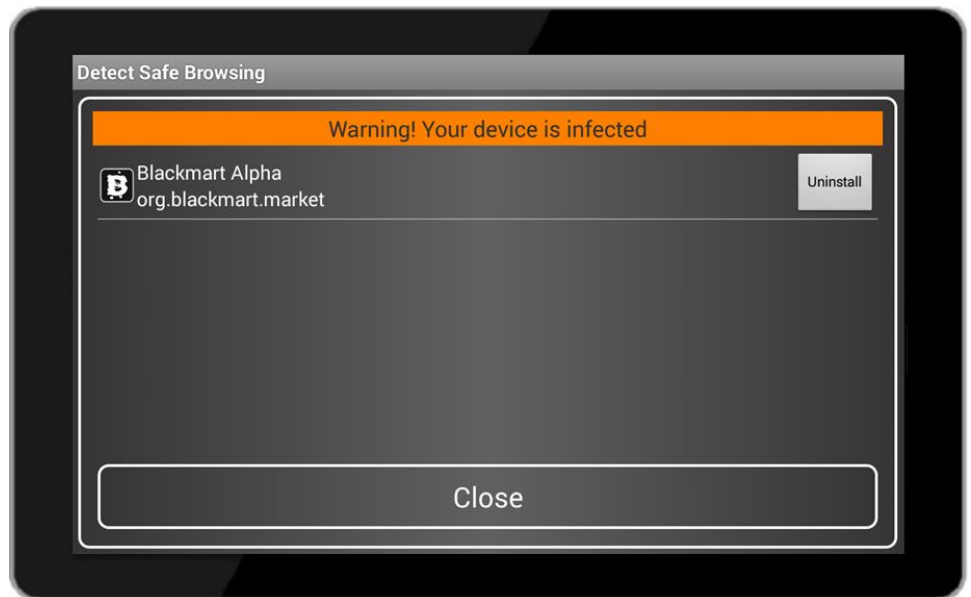
1. If the application does not find any suspicious activity, the following message will appear.



## DSB Console Operation

### Malware attacks

In case of detecting malware attacks, **Detect Safe Browsing** will inform you about the security threat:



- **Solution:**

**DSB** allows uninstalling any malicious applications found during a system analysis. Just press the button ***Uninstall*** on the right side of every entry.

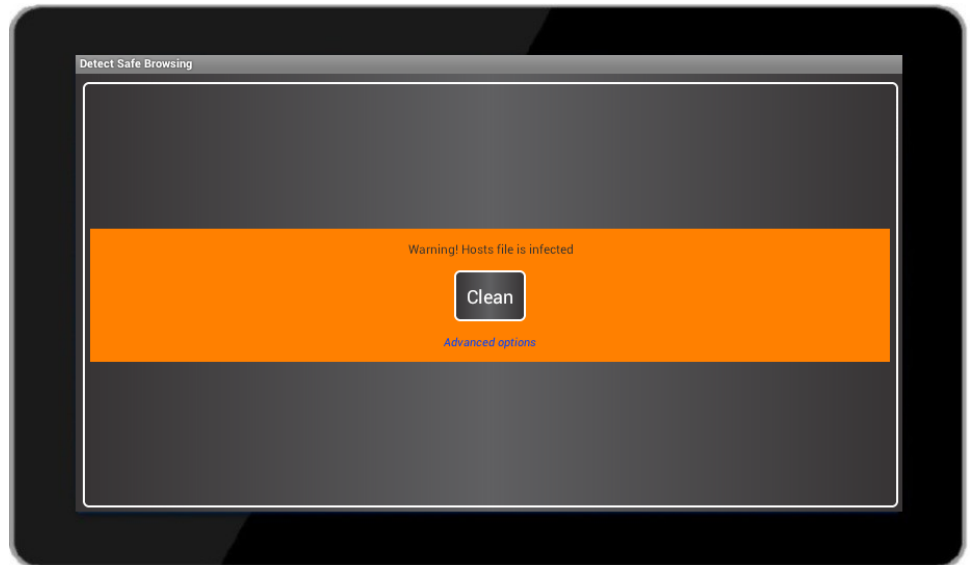




# DSB Console Operation

## Pharming attacks

In case of identifying pharming attacks, **Detect Safe Browsing** will block them and inform you about the threat:



- **Solution:**

You will be able to clean all suspicious URLs in your system directly through the DSB interface. Just press the button **Clean**:



**Note:** If you wish to keep certain entries in the *Hosts* file, you will be able to mark them as trustworthy. To do this, follow the steps in the section: [Marking suspicious URLs as trustworthy.](#)

# DSB Console Operation

*Marking suspicious entries as trusted*

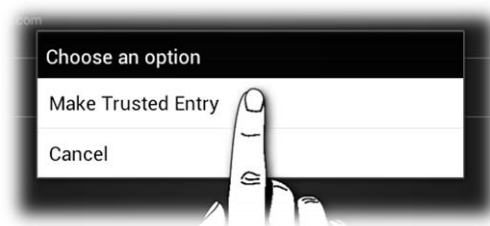
1. To unblock entries classified as suspicious, first scan your device:



2. Once the scanning process is complete, press the button **Advanced Options**:

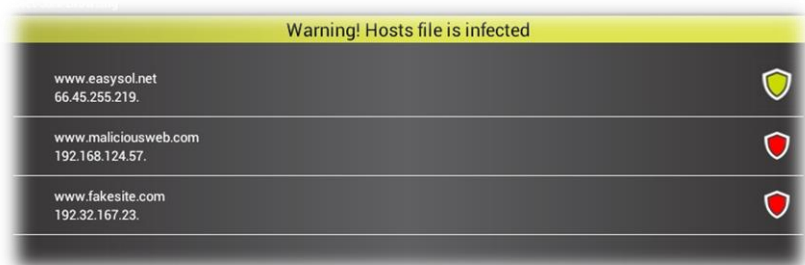


3. A detailed list of all malicious entries found in the *Hosts* file will appear. Press and hold the entry you wish to unblock and then press **Make Trusted Entry** on the pop up menu.

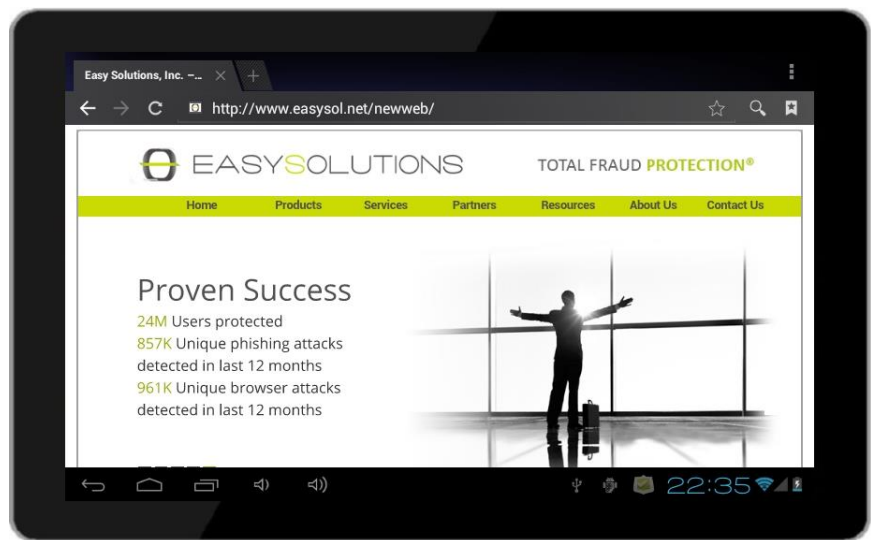


4. This entry will be classified as *Trusted* and its icon will switch to green.

# DSB Console Operation



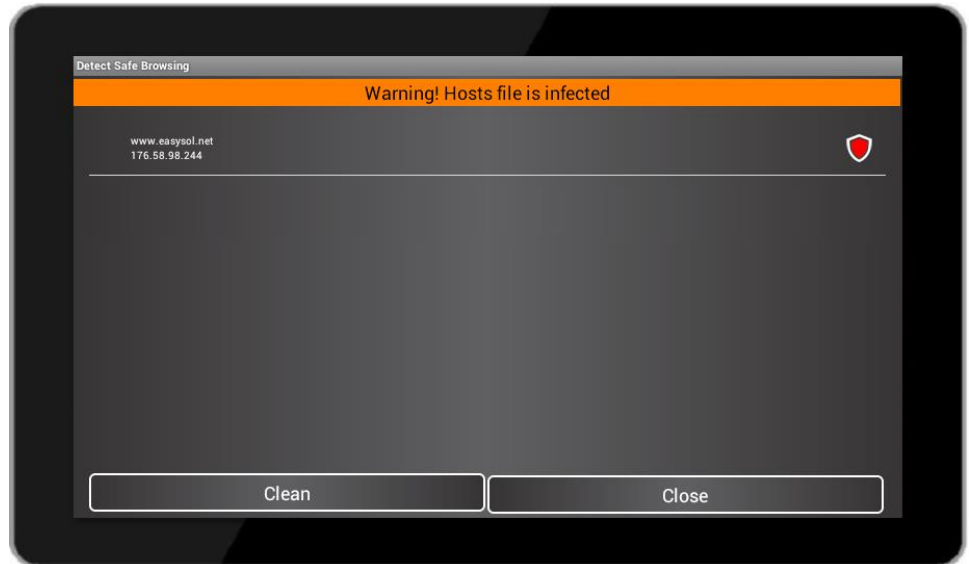
5. Now you can access this URL normally.



# DSB Console Operation

## *Cleaning your device*

1. Press the button **Clean** to delete all suspicious entries (marked with a red icon).



2. The threats will also be automatically reported to EasyLabs. To configure notification sending, please see **Configuring DSB**.

# DSB Console Operation

## Reports

Once **DSB** analyzes your system, it will record the events in a report calendar. Follow the steps below to consult it:

1. Select the option **Status** [1] to open the monthly record where you will see: the number of visits to protected websites (green icon) [2], and the number of malicious entries detected during that month (red icon) [3].



2. By pressing on any of the months, a list with the detailed information about the events recorded on that period of time will be displayed.



- **Red shield:** Security incident identified in the system.
- **Green shield:** Safe access to the [Protected Sites](#).

# DSB Console Operation

## *Protected Sites*

The Protected Sites are a set of web addresses that are protected by **Detect Safe Browsing** while browsing, ensuring their authenticity.

**Note:** **Detect Safe Browsing** for **Android** is compatible with the operating system's web browser.

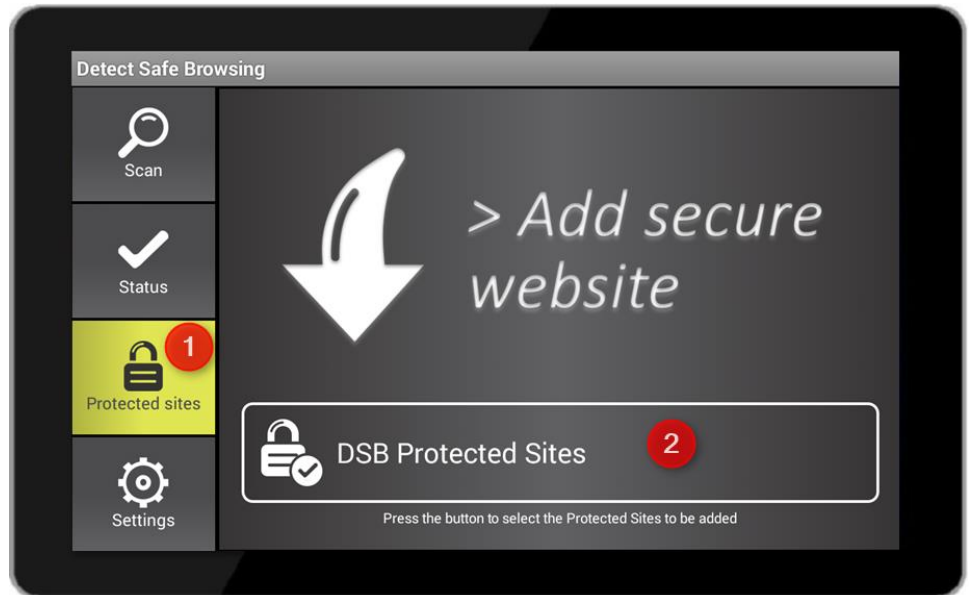
**DSB** has two types of Protected Sites:

- **Predefined by Easy Solutions** (🔒): Websites included by default in DSB. You won't be able to modify or delete them.
- **Personal** (🔒): Added by the end user. You will be able to modify or delete them.

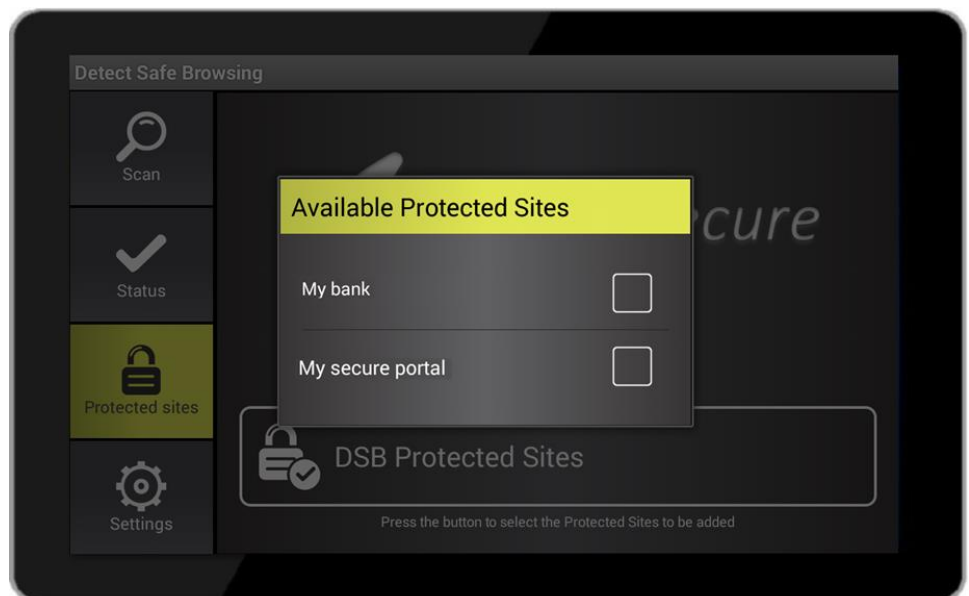
# DSB Console Operation

*Adding predefined protected websites*

1. In the menu *Protected Websites* [1], press the button *DSB Protected Websites*[2].

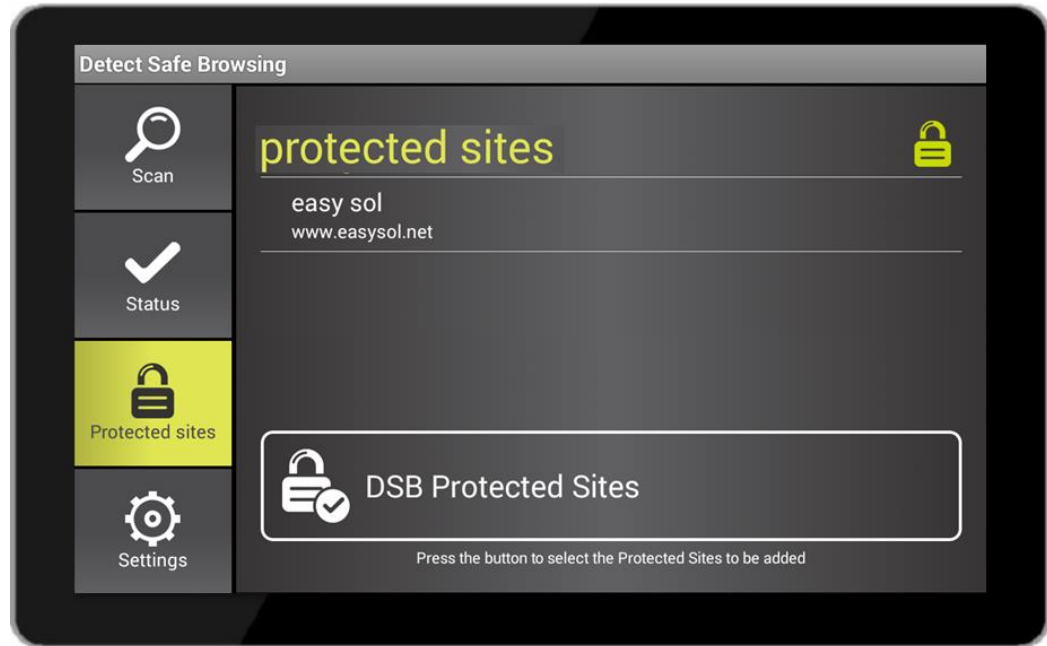


2. In the pop up window, check the boxes of the companies whose websites will be included in the DSB interface.



3. These websites will be added to the **Protected Websites** list and from that moment they can be accessed through the DSB interface.

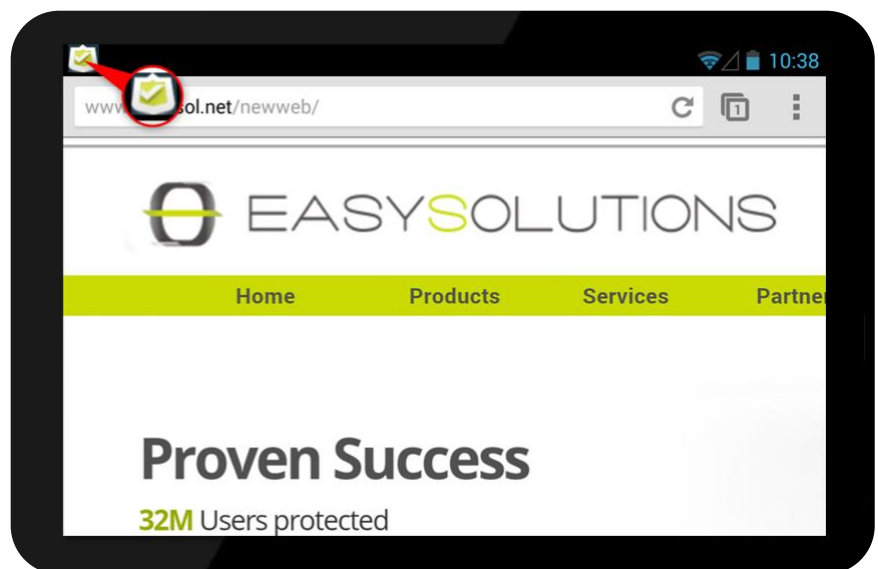
## DSB Console Operation



### *Adding personal protected websites*

To add a website to the **Protected Websites** list using the operating system's browser or Google Chrome:

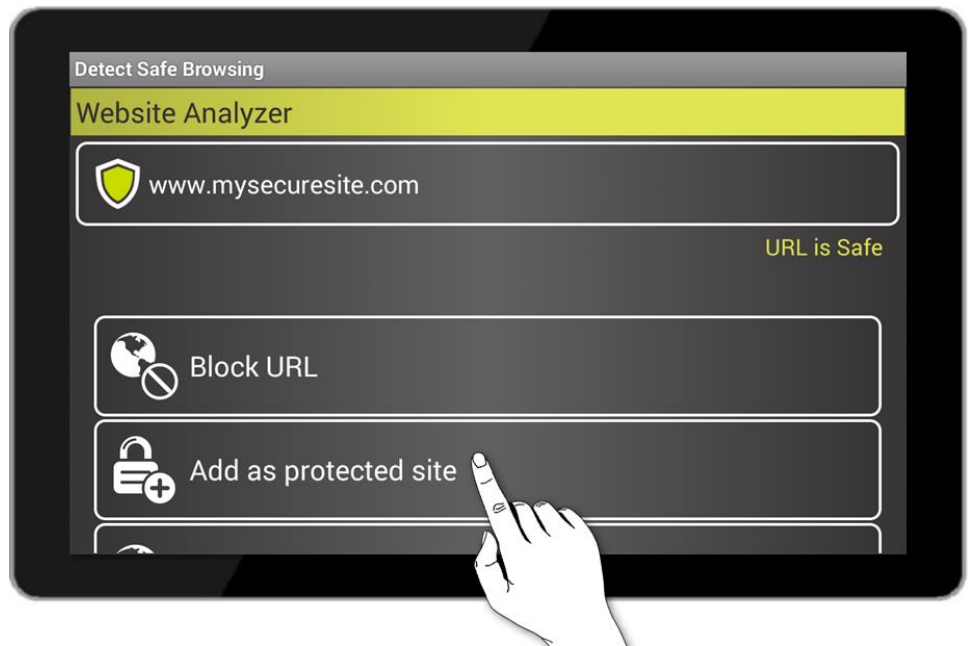
1. Open the notifications bar and press the **Detect Safe Browsing** icon.



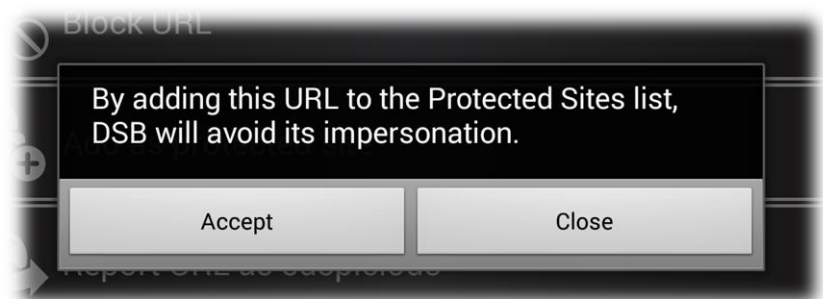
2. Press the option **Add to Protected Websites** (available only when browsing websites).



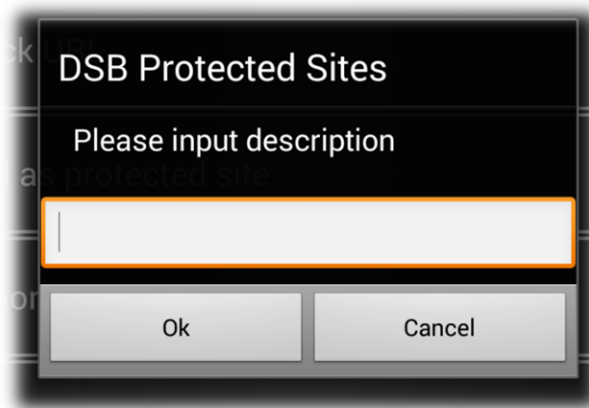
## DSB Console Operation



3. A confirmation message will appear, press **Accept**.

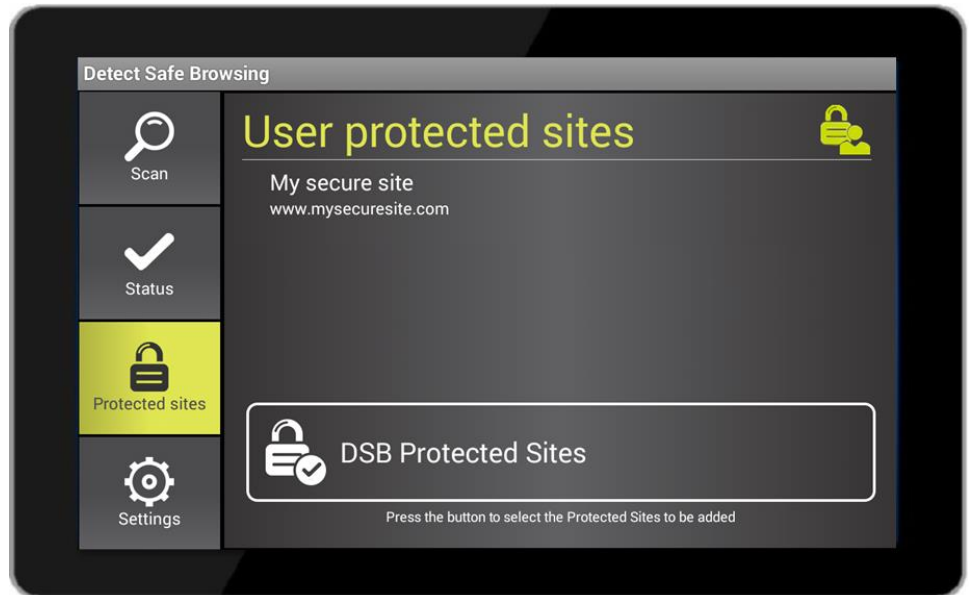


4. Next, you can add a brief description to identify this website:



## DSB Console Operation

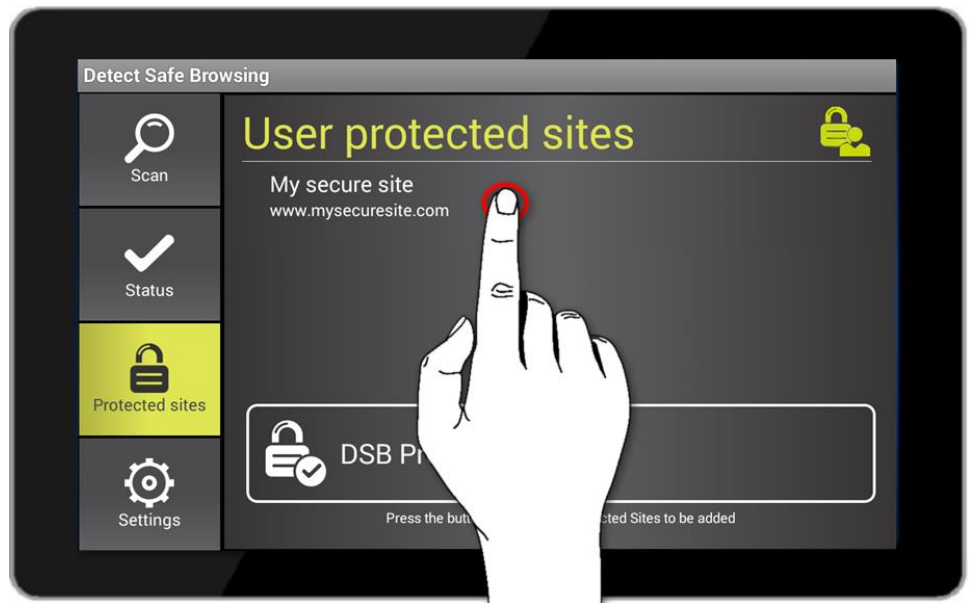
5. This website won't be blocked or reported as suspicious unless removed from the list.



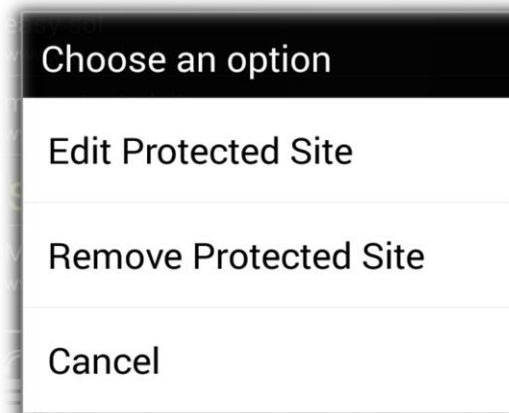
## DSB Console Operation


### *Editing protected websites*

6. In the **Protected Websites** menu, press and hold the website you wish to modify.



7. In the pop up menu, press **Edit Protected Site**.



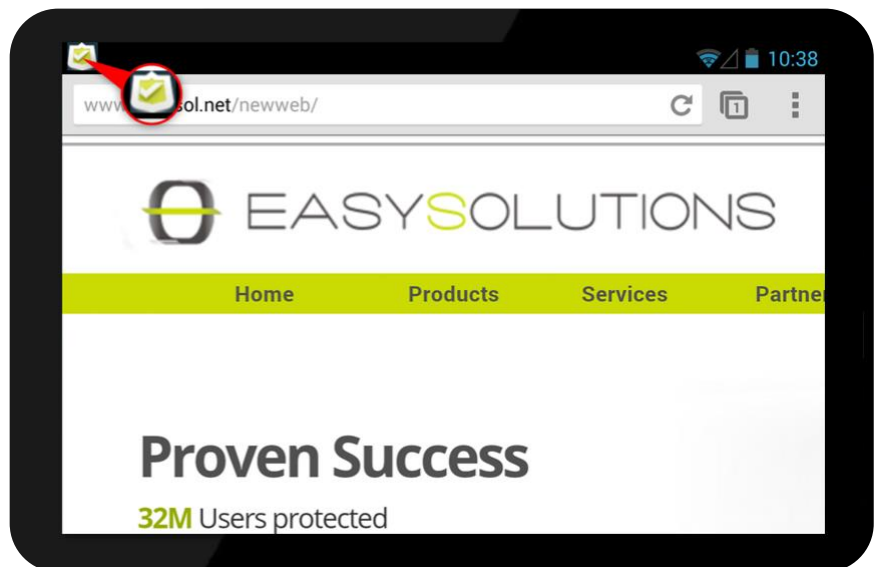
**Note:** Remember, you can only modify or delete personal protected websites. .

## 3 Web Protection

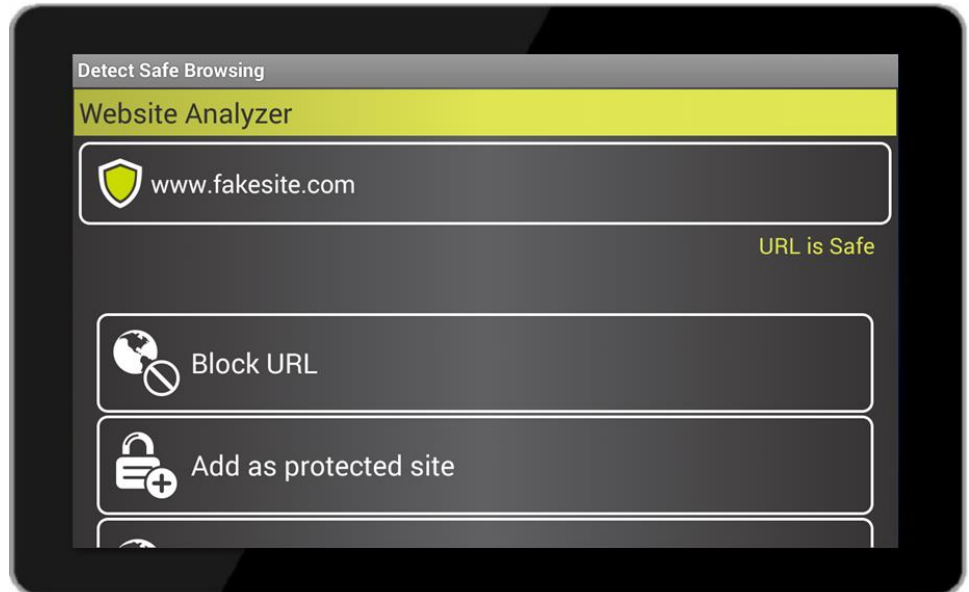
Another security strategy developed by Detect Safe Browsing for Android consists of the possibility to block, add as a protected site, or report the websites that you are currently visiting through the Internet browser of the operating system.

### Web Address




1. While browsing a website, open the notifications bar and tap on the **DSB Web Protection** icon.



2. At the top of the screen, you will find the URL of the site you are currently visiting.



Next to the visited URL, you will find one of the following notification icons:

Status	Icon
Website blocked by the user.	
Website unblocked by the user.	
Protected Site.	

The detailed procedures to run and perform the tasks mentioned above are described in the subsequent sections.

## Web Protection

### Reporting a URL

If you find suspicious or unreliable websites while browsing the Internet via the system browser, you can report them by following the steps below:

1. Tap on the *Report URL as suspicious* option, only available when browsing or accessing a website that is not in the Protected Sites list.



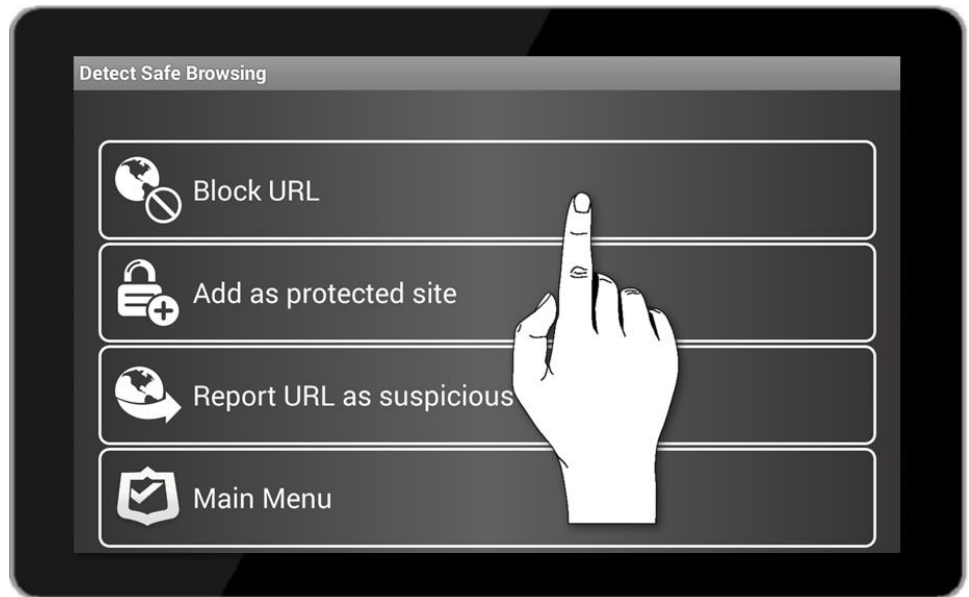
2. A confirmation message will be displayed; tap on the *Accept* option.



3. This URL will be sent to the **Easy Solutions** laboratories in order to be analyzed by our support team.

## *Blocking a URL*

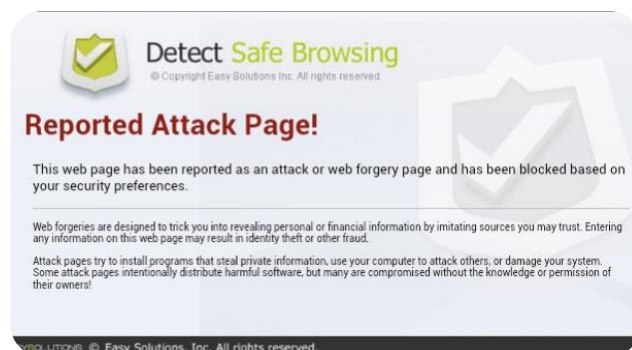
1. Tap on the *Block URL* option, only available while browsing.



2. A confirmation message will be displayed; tap on the *Accept* option.



3. Automatically, you will be re-directed to the operating system's web browser, where the following message will be displayed:



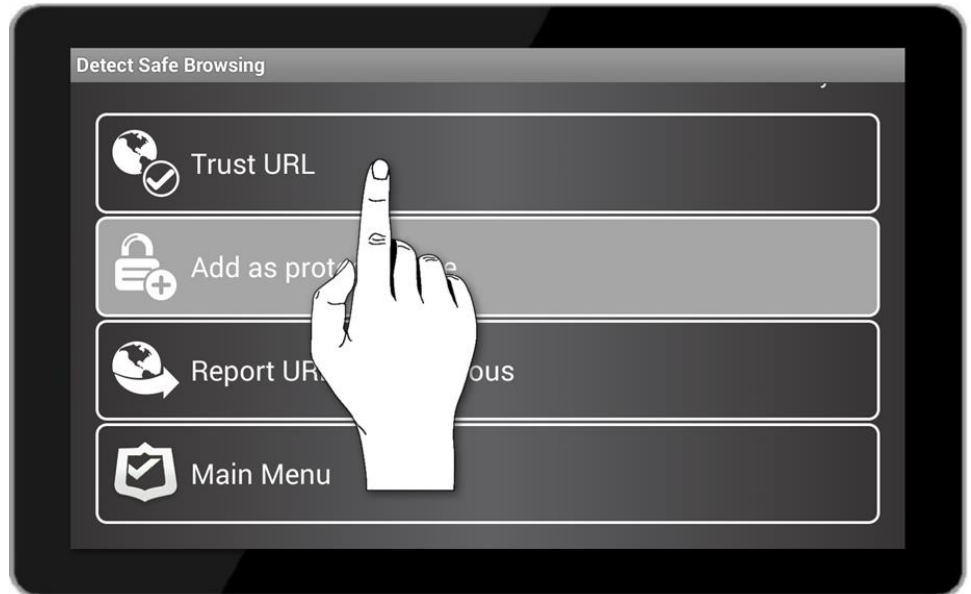
# Web Protection

## Unblocking a URL

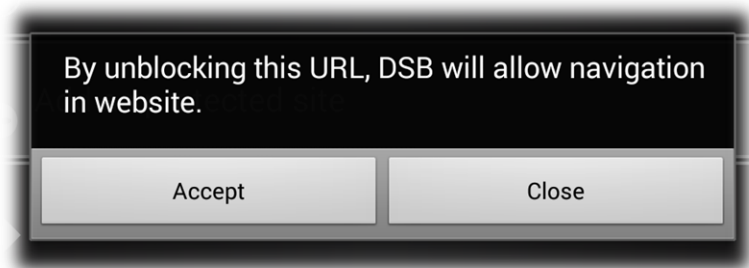
Before entering a website through the system's browser, **DSB** searches for the address in the URL Black List of the **Easy Solutions** servers. If the search matches any record in the list, the URL will be blocked immediately.

If you want to unblock the access to any of these URLs:

1. Tap on the *Trust URL* option, only available while browsing.



2. A confirmation message will be displayed; tap on the *Accept* option.



3. To consult the unblocked URLs, please go to the [Sites unblocked by the user](#) section.



# Web Protection

## Accessing the Main Menu

1. Press the *Main Menu* option to return to the DSB application.



2. DSB will open the main menu.

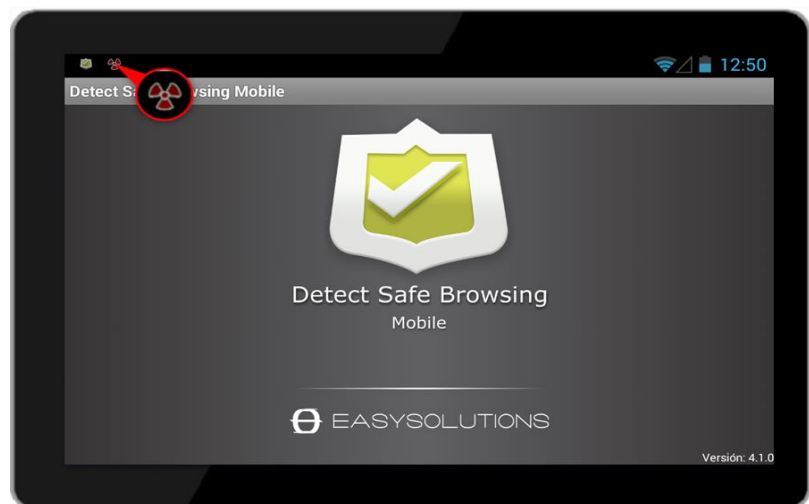
## 4 Monitoring applications

DSB constantly analyses the content of installed application in search of:

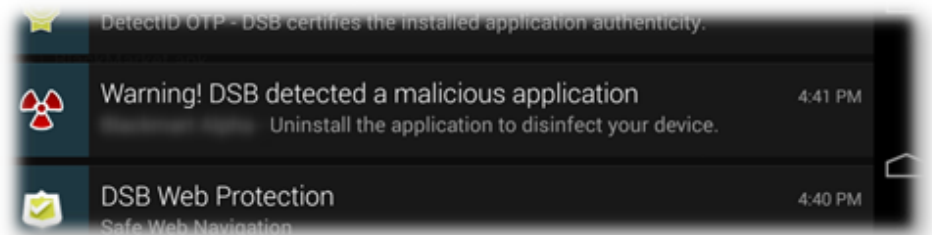
- **Malware attacks:** DSB will notify you about malicious content and allow uninstalling the application.
- **DSB-certified applications:** DSB will notify you about the authenticity of the application and its content.

### Malware notifications

Once an application is installed, DSB analyses its content and, in case of malware, the following icon will appear on the notifications bar:

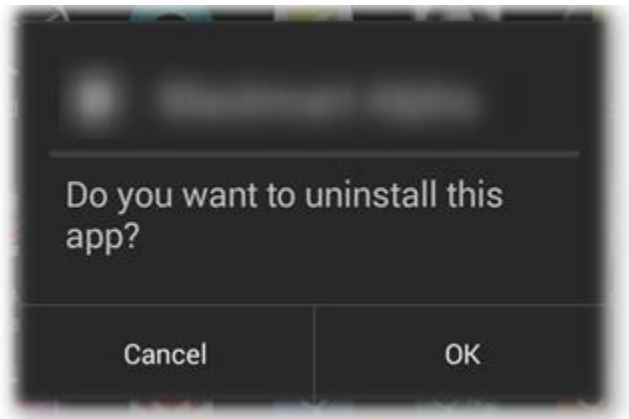


By opening the notifications bar, you will know more details about the threat.



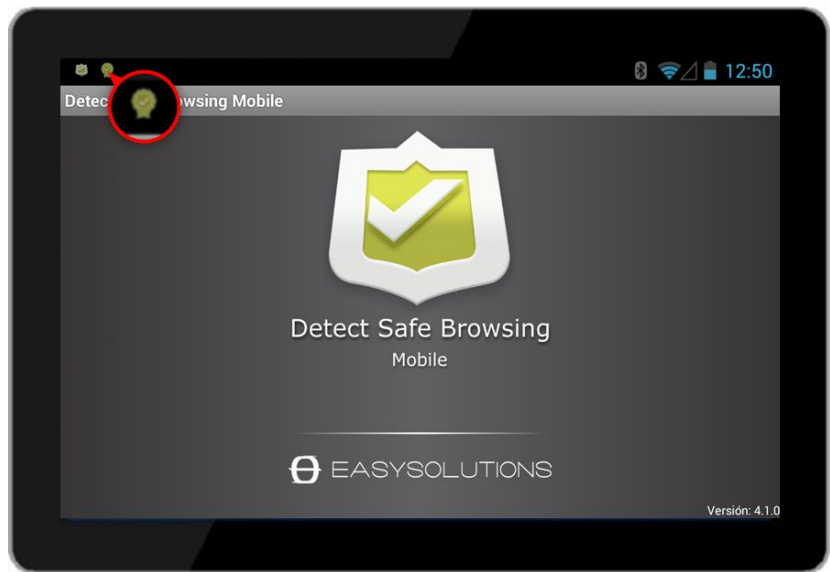
Pressing the notification will take you directly to the uninstallation assistant.

## Monitoring applications

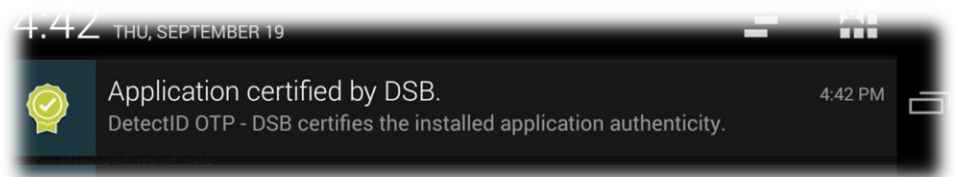


### *Certified application notifications*

Once an application is installed, DSB analyses its content and, if legitimate, the following icon will appear on the notifications bar:



By opening the notifications bar, you will know more details about the DSB certified application.



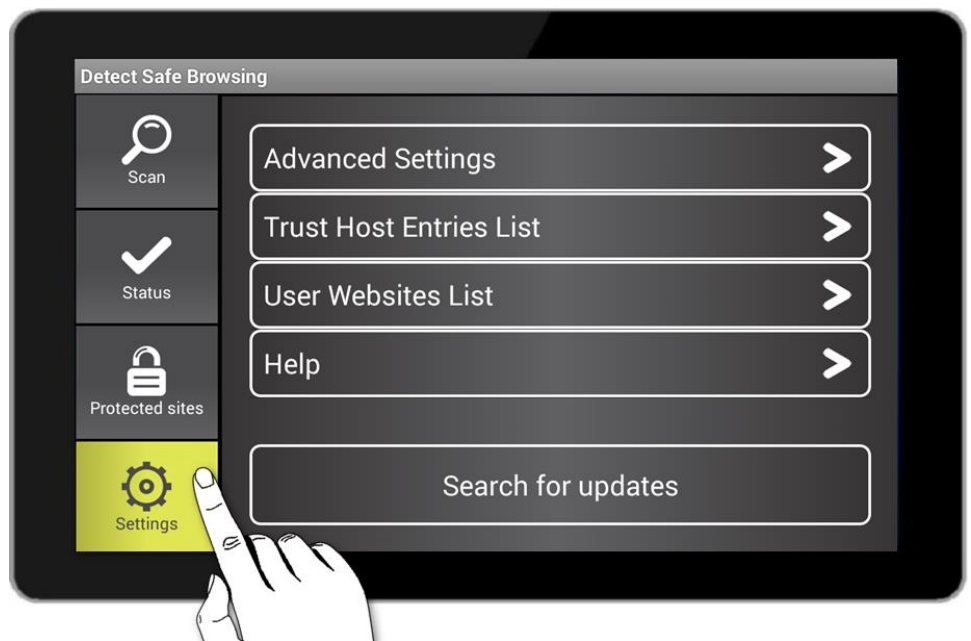
# 5

## Application Configuration

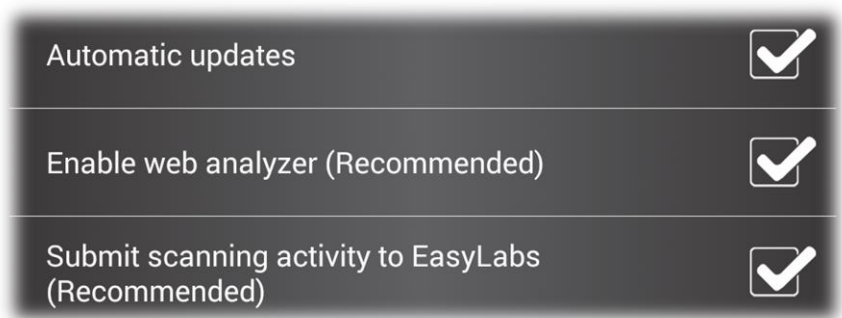
**Detect Safe Browsing** has many options that allow you to configure the application.

### Advanced Settings

1. Press the *Settings* option in the main menu.



2. Press the *Advanced Settings* option.



- **Automatic updates:** The DSB URL Black List will be updated hourly by enabling this option. In order to look for updates manually, tap on the

## Application Configuration

*"Search for updates"* option, located in the lower part of the window.

- **Enable Web Analyzer:** This functionality blocks Phishing attacks when the user attempts to enter a website that has been reported as malicious. Every time the user goes to any of these sites, the following message will be displayed when avoiding the attack.
- **Submit scanning activity to EasyLabs:** This option allows you to submit anonymous information about the events collected during the scanning process in order to be analyzed by the **Easy Solutions** laboratories.

# Application Configuration

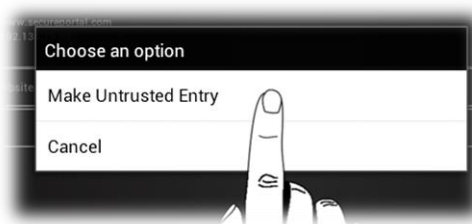
## Trusted entries in the Host file

Websites that were detected during the system scanning process and classified as trusted by the user. For further information, please see the [Pharming attacks](#) section.

1. Press the Settings option in the main menu.
2. Press the Trust Host Entries List option.



3. Then, you will find the entries previously identified as trusted. If you want to classify an entry as untrusted, tap and hold it and select the Make Untrusted Entry option.



4. If you want to remove the suspicious site from your system completely, repeat the [Scanning](#) process previously detailed in this manual.

## Sites unblocked by the user

Websites that were unblocked by the user while browsing the web (see [Unblocking a URL](#)). To consult this list:

1. Tap on the Settings option in the main menu.
2. Select the User Websites List option.



## Application Configuration

3. If you want to block this address again, press and hold the URL and select ***Remove URL from user Websites.***

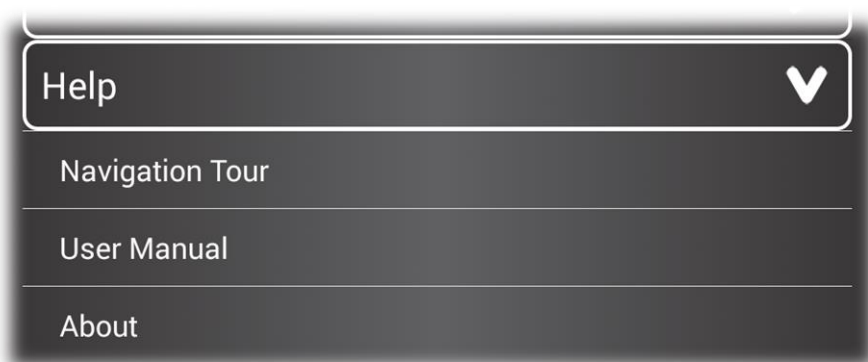


4. This website will be blocked by DSB.

# Application Configuration

## Help

1. Press on the **Settings** option in the main menu.
2. Press the Help option. You will see two orientation mechanisms ready to improve your Detect Safe Browsing for Android experience. These are the **Navigation Tour** and the **User Manual**.



## Version

If you want to know more about the Detect Safe Browsing version, press the **About** option in the **Settings** menu.

